Deutscher Bundestag **Drucksache 19/10307**
19. Wahlperiode 17.05.2019

Kleine Anfrage

der Abgeordneten Manuel Höferlin, Stephan Thomae, Benjamin Strasser, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marco Buschmann, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Otto Fricke, Katrin Helling-Plahr, Markus Herbrand, Katja Hessel, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Thomas L. Kemmerich, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Carina Konrad, Konstantin Kuhle, Ulrich Lechte, Michael Georg Link, Alexander Müller, Roman Müller-Böhm, Frank Müller-Rosentritt, Dr. Martin Neumann, Bernd Reuther, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Frank Sitta, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Katja Suding, Linda Teuteberg, Michael Theurer, Nicole Westig, Katharina Willkomm und der Fraktion der FDP

Nutzung externer Cloud-Anbieter und Aufbau eigener Cloud-Infrastrukturen durch die Bundesregierung

Die Bundespolizei speichert Bodycam-Aufnahmen in Amazons AWS-Cloud (vgl. Antwort der Bundesregierung auf die Schriftliche Frage 28 des Abgeordneten Benjamin Strasser auf Bundestagsdrucksache 19/8180). Nach Ansicht der Fragesteller sollten die Bundespolizei und die anderen deutschen Sicherheitsbehörden eigentlich sachlich und personell ausreichend ausgestattet sein, um solche sensiblen Daten auch ohne externe Anbieter auf dem nötigen Sicherheitsniveau zu speichern und zu verarbeiten. Laut der Antwort der Bundesregierung auf die Mündliche Frage 34 des Abgeordneten Konstantin von Notz (vgl. Plenarprotokoll 19/88) kommt allerdings durch die ausgewählte Hardware des Anbieters Motorola und die auf die Hardware abgestimmte Cloud-Architektur allein AWS als Cloud-Dienst in Betracht. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber, hält die Speicherung von Bodycam-Daten in der Amazon Cloud für rechtswidrig und forderte die Bundesregierung auf, zu einem deutschen Cloud-Anbieter umzusteigen (Quelle: www.noz.de/deutschland-welt/politik/artikel/1685384/bundespolizei-geraet-wegen-speicherung-von-bodycam-aufnahmen-unter-druck).

Das Informations Technik Zentrum Bund (ITZBund) lässt momentan die sogenannte Bundescloud entwickeln. Aus der dazugehörigen Ausschreibung „Software und Dienstleistungen für die Bundescloud“ aus dem Jahr 2016 geht hervor, dass die Bundescloud zunächst für bis zu 350 000 Nutzer ausgestaltet werden,

aber weiter skalierbar sein soll. Die Bundescloud soll für ihre Nutzer als „BCBox“ angeboten werden (Quelle: www.itzbund.de/Restricted/DE/Ausschreibungen/O1912-Z4-1519-2017/Download_Vergabeunterlagen.html).

Auf dem Digitalgipfel der Bundesregierung 2018 in Nürnberg wurde die digitale Souveränität als Regierungslinie verabschiedet (Quelle: www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5). Digitale Souveränität wird in mehreren Kontexten auf das Prinzip der eigenständigen Handlungsfähigkeit in verschiedenen Bereichen der Digitalisierung zurückgeführt, unter anderem in den Bereichen Staat und Verwaltung. Bedenkt man dies, so wirft nach Ansicht der Fragesteller generell die Nutzung von externen Anbietern für Cloud-Dienste durchaus Fragen auf.

Im Jahr 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Anforderungskatalog Cloud Computing (C5) herausgegeben, der als Prüfstandard für Cloud-Dienste gelten soll. Das Bundesministerium für Wirtschaft und Energie (BMWi) war (Mit-)Initiator des Trusted Cloud Labels und des Prüfstandards „Trusted Cloud Datenschutz-Profil für Cloud-Dienste“ (TCDP). Das Trusted Cloud Label wird vom Kompetenznetzwerk Trusted Cloud e. V. herausgegeben und verwaltet, das TCDP von der Stiftung Datenschutz.

Wir fragen die Bundesregierung:

1. In welchen Bereichen nutzt die Bundesregierung, unter anderem für die Sicherheitsbehörden, externe Anbieter für Cloud-Dienste?

   a) Welche Anbieter werden in den jeweiligen Bereichen genutzt?

   b) Welche Aufgaben werden genau an die Anbieter ausgelagert (beispielsweise laufender Betrieb, Archiv etc.)?

   c) Werden Software-, Plattform- oder Infrastruktur-Dienste (SaaS, PaaS oder IaaS) verwendet?

      Welche dieser Dienste-Kategorien werden in welcher Form bei der Verwendung der AWS-Cloud durch die Bundespolizei genutzt?

2. Welche der Cloud-Dienste werden aufgrund eigenständiger Verträge mit den Anbietern genutzt, welche der Dienste werden im Zusammenhang mit einer angeschafften Hard- bzw. Software-Lösung oder bereits bestehenden Rahmenverträgen genutzt?

3. Warum hat sich die Bundesregierung in den jeweiligen Konstellationen für die Nutzung externer Anbieter und gegen die Nutzung eigener Speicherinfrastruktur entschieden (bitte die einzelnen Bereiche und Nutzungsfälle externen Anbieter auflisten)?

   a) Lag es mehrheitlich eher an fehlender eigener Speicherinfrastruktur oder an fehlendem Know-how in der Bundesregierung?

   b) Warum war in den jeweiligen Fällen die „Bundescloud“ des ITZBund nicht als Speicherort geeignet, oder aus welchen anderen Gründen wurde diese nicht ausgewählt?

4. Welche Verträge wurden durch Ausschreibungen vergeben (bitte jeweiligen Link zur Ausschreibung angeben)?

   a) In welchem Verfahren wurden die übrigen Aufträge vergeben?

   b) Welche Ausschreibungen zur Vergabe sind noch geplant?

   c) Welches sind die verfahrensleitenden Kriterien der Bundesregierung für die Ausschreibung von Cloud-Diensten?

5. Welche Kriterien gibt es, um kritische und sensible Daten nicht zur Speicherung und Verwendung an einen Cloud-Anbieter auszulagern?

   Welche Daten gelten aus Sicht der Bundesregierung als kritisch oder sensibel?

6. Wie schätzt die Bundesregierung die Relevanz von Meta-Daten im Kontext von Cloud-Diensten ein?

   a) Wie wird sichergestellt, dass kein unbefugter Zugriff auf Meta-Daten bei den verwendeten externen Anbietern stattfindet?

   b) Welchen Zugriff und welche Nutzung bzw. Verwertung von Meta-Daten erlaubt die Bundesregierung den momentan genutzten externen Cloud-Anbietern?

   c) Wie ist der Zugriff auf Meta-Daten mit den jeweiligen Anbietern geregelt?

7. Setzt die Bundesregierung bei der Nutzung ihrer Cloud-Dienste (eigene und externe) intelligente Such- und Erkennungssysteme, z. B. unter Einsatz von Künstlicher Intelligenz (KI), ein?

   a) Falls ja, verwendet die Bundesregierung hierfür eigens erstellte oder selbst angeschaffte KI-Anwendungen oder verwendet die Bundesregierung von den externen Anbietern bereitgestellte KI-Anwendungen?

   b) Falls ja, wie stellt die Bundesregierung sicher, dass die externen Anbieter nicht für eigene Zwecke KI-Anwendungen nutzen, um die gespeicherten Daten oder deren Meta-Daten auszuwerten?

8. Wie stellt die Bundesregierung sicher, dass die auf externe Cloud-Dienste ausgelagerten Daten die nötige Mobilität (beispielsweise durch Schnittstellen) besitzen?

   a) Welche Vorkehrungen wurden getroffen, um ggf. den Anbieter ohne eine Dienstunterbrechung wechseln zu können?

   b) Wie wird darüber hinaus die Unabhängigkeit vom Anbieter sichergestellt?

   c) Inwiefern wird künftig bei der Anschaffung von Hardware oder anderer IT-Infrastrukturen sichergestellt, dass die Interoperabilität mit eigenen Cloud-Diensten gewährleistet ist?

9. Hält die Bundesregierung die Speicherung von Daten in der AWS-Cloud entgegen der Äußerung des BfDI Ulrich Kelber für rechtmäßig?

10. Wie stellt die Bundesregierung bei der Verwendung amerikanischer externer Anbieter technisch und rechtlich sicher, dass die durch den CLOUD Act bestehenden Befugnisse nicht dazu verwendet werden, Daten in die USA zu übertragen?

    Wie wird dies konkret im Falle der Verwendung von AWS sichergestellt?

11. Wird bei der Verwendung von Office-Anwendungen durch die Bundesregierung das Produkt „OneDrive“ von Microsoft genutzt?

    Falls ja,

    a) werden die Daten verschlüsselt?

    b) wie werden Meta-Daten geschützt?

    c) wie wird technisch und rechtlich sichergestellt, dass keine unrechtmäßigen Datenübertragungen in Drittländer stattfinden?

12. Wurde nach Kenntnis der Bundesregierung bei der Beschaffung der Bodycams durch die Bundespolizei auch die Softwarelösung zur Verwaltung der entstehenden Daten evaluiert?

    a) Gab es für die Auswahl einer geeigneten Lösung Ausschlusskriterien in Bezug auf die Verwaltungssoftware für die Daten?

       War beispielsweise die Möglichkeit zur Verarbeitung biometrischer Daten ein solches Kriterium?

    b) Wurde die Möglichkeit einer späteren Migration der angefallenen Daten in eine eigene Speicher-Infrastruktur (beispielsweise die „Bundescloud“) evaluiert?

       Schätzt die Bundesregierung dies als technisch möglich ein?

       Wie viel würde eine solche Migration nach Einschätzung der Bundesregierung kosten?

       Wurde für diesen Zweck ein Fixpreis mit dem Anbieter vereinbart?

13. Auf welchen Ebenen und an welchen Stellen werden nach Kenntnis der Bundesregierung derzeit staatliche Cloud-Infrastrukturen auf- oder ausgebaut?

    a) In welchem Umfang sind diese geplant?

    b) Wann sollen diese fertiggestellt sein?

    c) An welcher Stelle sind entsprechende Projekte der Bundesregierung in der Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels zu finden?

14. Wie weit ist die Entwicklung der „Bundescloud“ fortgeschritten?

    An welchen Nutzerkreis soll sich die „Bundescloud“ und die Anwendung „BCBox“ richten?

    Zu welchem Zweck sollen die Anwendungen verwendet werden können?

15. Wird die Bundescloud nur verwaltungsintern Verwendung finden?

    Oder wird die Bundescloud auch im Rahmen der Digitalisierung der Verwaltungsleistungen zur Anwendung kommen?

16. Wurde der C5-Prüfstandard vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt?

    Wenn nein, von wem wurde dieser entwickelt?

    Wurden vom BSI hierzu externe Dienstleister in Anspruch genommen?

    Wenn ja, welche?

17. Wurden die Kriterien für das Trusted Cloud Label und den TCDP-Prüfstandard durch das BMWi entwickelt?

    Wenn nein, von wem wurden diese entwickelt?

    Wurden vom BMWi bzw. dem Kompetenznetzwerk Trusted Cloud e. V. und der Stiftung Datenschutz hierzu externe Dienstleister in Anspruch genommen?

    Wenn ja, welche?

18. Wie viele und welche Anbieter sowie einzelne Cloud-Dienste sind nach Kenntnis der Bundesregierung nach dem Trusted Cloud Label oder dem C5- und TCDP-Prüfstandard zertifiziert?

    a) Werden die Zertifizierungen nach dem Trusted Cloud Label durch das Kompetenznetzwerk Trusted Cloud e. V. vorgenommen?

       Falls ja, wie viel Budget ist in welchem Einzelplan an welcher Stelle für das Haushaltsjahr 2019 hierfür eingeplant?

       Falls nein, wer übernimmt die Zertifizierungen, und welche Kosten verursacht dies für die öffentliche Hand?

    b) Werden die Zertifizierungen nach dem TCDP-Prüfstandard durch die Stiftung Datenschutz vorgenommen?

       Falls ja, wie viel Budget ist in welchem Einzelplan an welcher Stelle für das Haushaltsjahr 2019 hierfür eingeplant?

       Falls nein, wer übernimmt die Zertifizierungen, und welche Kosten verursacht dies für die öffentliche Hand?

    c) Werden die Zertifizierungen nach dem C5-Prüfstandard durch das BSI vorgenommen?

       Falls ja, wie viel Budget ist in welchem Einzelplan an welcher Stelle für das Haushaltsjahr 2019 hierfür eingeplant, und wie viele Planstellen sind hierfür vorgesehen?

       Falls nein, wer übernimmt die Zertifizierungen, und welche Kosten verursacht dies für die öffentliche Hand?

Berlin, den 8. Mai 2019

Christian Lindner und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333